Central Bank of Nigeria

Financial Policy & Regulation Department
Plot 33, Abubakar Tafawa Balewa Way
Central Business District
P.M.B. 0187 Garki, Abuja - Nigeria.
E-mail: fprd@cbn.gov.ng
Website: www.cbn.gov.ng
Phone: +234 700-225-5226, +234 800-225-5226

FPR/DIR/PUB/CIR/001/010

November 26, 2025

CIRCULAR TO ALL BANKS, OTHER FINANCIAL INSTITUTIONS, PUBLIC INTEREST GROUPS, AND THE PUBLIC

DRAFT GUIDELINES FOR HANDLING AUTHORISED PUSH PAYMENT FRAUD

The Central Bank of Nigeria, in furtherance of its mandate of promoting a sound financial system in Nigeria, hereby exposes this draft Guidelines aimed at addressing the rising incidence of Authorised Push Payment fraud in the financial system for comments.

When finalised, the Guidelines would mandate all financial institutions to institute preventive measures as well as modalities for mitigating and managing APP fraud.

Banks, other financial institutions, public interest organisations, and the general public are invited to submit their comments on the draft Guidelines in softcopy to coanene@cbn.gov.ng, asojie@cbn.gov.ng, and nakagworo@cbn.gov.ng, not later than three weeks from the date of this circular.

DR. RITA I. SIKE
DIRECTOR, FINANCIAL POLICY & REGULATION DEPARTMENT

CENTRAL BANK OF NIGERIA

DRAFT GUIDELINES FOR HANDLING AUTHORISED PUSH PAYMENT FRAUD

EXPOSURE DRAFT

NOVEMBER 2025

Contents

EXPOSURE DRAFT

GLOSSARY

For the purpose of this Guidelines, the following terms will have the meanings assigned hereunder:

S/N	TERM	MEANING
1	Criminal intent	The deliberate or conscious decision to engage in actions that constitute or facilitate APP fraud, with the knowledge that such actions are unlawful
2	Financial Institutions	Entities licensed by the Central Bank of Nigeria to render financial services. They include, but are not limited to commercial, merchant, non-interest, payment service, microfinance, and primary mortgage banks, finance companies, mobile money operators, and payment service providers. The term is used interchangeably with banks and other financial institutions (OFIs) in this Guidelines.
3	Inducement	An act of persuading, influencing, or enticing an individual through deception, misrepresentation, or undue advantage to authorise or initiate a payment or transaction that results in financial loss or facilitates an APP fraud incident
4	Negligence	Failure by a financial institution, its staff, or customer to exercise the level of care, diligence, or prudence that a competent person would ordinarily be expected to exercise in similar circumstances, thereby resulting in or contributing to an APP fraud incident
5	No reasonable cause to suspect fraud	A determination that, based on the circumstances of the transaction and available evidence, a prudent person would not have had sufficient grounds to believe that a transaction was fraudulent at the material time
6	Red flagged account	An account identified through transaction monitoring, investigation, or intelligence as exhibiting suspicious characteristics, unusual patterns, or behaviour commonly associated with fraudulent activities, thereby warranting enhanced scrutiny or temporary restriction pending further review
7	Reimbursement	The act of refunding or compensating a customer for financial loss incurred due to an APP fraud incident, subject

EXPOSURE DRAFT

		to the conditions and eligibility criteria stipulated in this Guidelines
8	Staff collusion	Any act where an employee or representative of a financial institution knowingly assists, conspires, or otherwise participates, directly or indirectly, in the commission or concealment of an APP fraud incident

EXPOSURE DRAFT

1.0. INTRODUCTION

Over the years, Nigeria's financial system has witnessed the transformative impact of digital payment channels, including but not limited to mobile banking, Unstructured Supplementary Service Data (USSD), internet banking, and instant transfers, on Nigeria's financial ecosystem. These platforms have significantly enhanced efficiency, fostered financial inclusion, and provided unparalleled convenience for the banking public.

However, the rapid adoption of these digital channels has been accompanied by a surge in electronic fraud. These fraudulent activities not only result in direct financial losses for individuals and institutions but also erode public trust in the financial system, which is essential for a safe, sound and resilient financial system.

Among these fraudulent activities, Authorised Push Payment (APP) fraud has been a growing concern in the industry. Unlike traditional fraud where an account is compromised without the owner's knowledge, a customer is manipulated, persuaded, or misled to voluntarily make a payment to a third party's account, who has either impersonated a legitimate entity/individual or wilfully refused to fulfil an obligation. This form of fraud, often executed through social engineering methods, exploits the customer's trust and the finality of digital transactions, making it increasingly challenging to detect and prevent.

In line with its mandate to ensure a safe, sound and resilient financial system and its resolve to safeguard the integrity of the Nigerian payments system, the Central Bank of Nigeria (CBN/Bank) hereby issues this Guidelines in exercise of the powers conferred on it by the CBN Act, 2007 and the Banks and Other Financial Institutions Act (BOFIA), 2020.

The Guidelines should be read in conjunction with the CBN Act, the BOFIA, other relevant laws, subsidiary legislations made under the Acts, the CBN's Consumer Protection Framework, as well as written directives, notices, circulars and guidelines issued by the CBN.

EXPOSURE DRAFT

2.0. OBJECTIVES

This Guidelines aims to:

i. set out the minimum requirements and expectations for the prevention, detection, reporting, and/or resolution of APP fraud across digital payment channels,

ii. safeguard the integrity of the payment system,
iii. protect the interests of all stakeholders, and
iv. ensure that the benefits of digital innovation are realised without compromising public confidence.

3.0. SCOPE AND APPLICABILITY

This Guidelines applies to all financial institutions under the regulatory purview of the CBN and covers all electronic payment channels through which customers initiate push transactions, including but not limited to mobile banking applications, internet banking platforms, USSD services, and payment gateway interfaces.

4.0. AUTHORISED PUSH PAYMENT FRAUD

APP fraud shall include, but is not limited to:

i. Inducement, coercion or misleading of a user/customer into authorising a payment via WhatsApp, SMS, E-mails and any other communication channel to a third party's account or wallet.

ii. Facilitation, negligence, or non-compliance by financial institutions, such as failure to act on red flags, weak Know Your Customer (KYC) or fraud controls, staff collusion, delayed resolution, and use of accounts for fraudulent purposes.

5.0. GOVERNANCE

i. The Board of financial institutions shall have responsibility for the governance of APP fraud risk management; and for approval of the risk management and internal control policies and processes for the prevention, detection, mitigation, investigation, response, recovery, and post-incident review of APP fraud.

ii. The Board shall periodically review APP fraud trends, evaluate the effectiveness/resilience of controls as well as responses to APP fraud incidents.

iii. The Board shall formulate and implement APP fraud policy which shall, at a minimum, cover the following:

POSURE DRAFT

a. Scope of the policy;

b. Description of actions considered as APP fraud;

c. Roles and responsibilities of the Board, Board Risk Management Committee (BRMC), Board Audit Committee (BAC), Executive Director (Risk), Chief Risk Officer (CRO), Chief Compliance Officer and Head of Internal Audit as they relate to handling APP fraud;

d. Risk Assessment Process;

e. Measures for the prevention and detection of APP fraud;

f. Investigation and escalation procedures;

g. Recovery procedures;

h. Reimbursement;

i. Confidentiality;

j. Reporting Procedures;

k. Response & Remedial Measures;

l. Record-Keeping and Documentation;

m. Compliance and Legal Considerations;

n. Review/update of policy;

o. Collaboration and information-sharing with industry stakeholders and law enforcement agencies; and

p. Any other matter as may be required by the CBN.

iv. The APP fraud policy shall be reviewed at least once every two years.

v. The Board shall assign the oversight responsibility for the handling of APP fraud risk to the Board Risk Management Committee.

vi. The Board shall assign the oversight responsibility for investigation of APP fraud offences to the Board Audit Committee.

vii. The Head of Internal Audit shall provide the Board Audit Committee with a summary of all reported APP fraud cases and the result of their investigation.

viii. The Board shall designate the responsibility for the implementation of the provisions of this Guidelines to the Head of Compliance.

6.0. RISK MANAGEMENT

To promote proactive fraud risk management, financial institutions shall at a minimum, implement Early Warning System (EWS) for the prevention and/or timely detection and mitigation of APP fraud. Such measures may include red flagging accounts on suspicion of fraudulent activities, behavioural monitoring, and documentation of EWS indicators (such as accounts identified through fraud typologies, repeated complaints, unusual inflows/outflows, or previous involvement in fraud cases). These accounts shall be subjected to enhanced monitoring and/or restricted pending investigation.

Banks and OFIs shall:

i. Implement EWS for the timely detection and mitigation of APP fraud, incorporating red flagging of accounts suspected of fraudulent activities.

ii. Ensure that EWS indicators shall be thoroughly documented, including but not limited to, accounts identified through fraud typologies, repeated complaints, unusual inflows/outflows, or prior involvement in fraud cases.

iii. Accounts flagged under the EWS shall be subject to enhanced monitoring and/or restriction pending a full investigation.

iv. Establish a Board-approved framework for EWS and Red Flagging of Accounts (RFA) specifically for APP fraud.

v. The EWS shall:

EXPOSURE DRAFT

a. be comprehensive, integrating both quantitative and qualitative indicators to ensure its robustness and effectiveness; and

b. capture broad indicators derived from transactional data, customer financial performance, market intelligence, and customer conduct.

vi. Financial institutions shall have a unit with responsibility for fraud data analytics. The resources allocated to the unit shall be appropriate to the institution's size, complexity, and risk profile to facilitate collection and processing of relevant information for prevention and early detection of potentially fraudulent activities.

vii. All EWS alerts and triggers shall be promptly examined to determine the necessity for red flagging account(s) and for initiating further investigation on potential fraudulent activities.

viii. Banks shall continuously review and strengthen their EWS, to enhance its effectiveness and robustness in monitoring all credit and non-credit related transactions towards the prevention of fraudulent activities through banking channels.

ix. Financial institutions shall test the effectiveness of their EWS at least on a half-yearly basis to ensure its ongoing efficacy.

POSURE DRAFT

7.0. COMPLAINTS RESOLUTION

i. Banks and OFIs shall establish reporting mechanisms that allow customers to report APP fraud incidents through designated channels, including customer service hotlines, email, mobile applications and in person at any branch.

ii. The designated channels may include, emails, SMS/USSD options, mobile applications, official social-media handles, and a toll-free service hotline which shall support multiple languages. These channels shall be operational 24 hours a day, seven (7) days a week.

iii. Any customer who is a victim of APP fraud is expected to, within twenty-four (24) hours of the occurrence, report the incident to their financial institution using the designated channels. Notwithstanding this expectation, customers shall have up to an additional forty-eight (48) hours to make such a report.

iv. Financial institutions shall apply a higher duty of care when assessing the actions of customers who can be demonstrably classified as vulnerable.

v. The report shall contain sufficient information to aid investigation, including transaction date, amount, recipient account details, and any available supporting documentation.

vi. Upon receipt of the report from a customer, the financial institution shall ensure that a formal investigation into the alleged APP fraud is initiated immediately.

vii. Financial institutions shall acknowledge receipt of the report within twenty-four (24) hours and issue a unique case reference number to the customer and a summary of the review process, including indicative timelines for resolution.

viii. The CBN may direct NIBSS or any relevant settlement entity to withhold settlement for the full value of any transaction identified as fraudulent. This may extend to second level or other subsequent beneficiary institutions along the transaction chain.

ix. The full investigation shall be concluded within fourteen (14) working days, after which a clear decision shall be communicated to the customer.

x. Financial institutions shall clearly communicate the outcome of the APP fraud investigations to the customer stating if reimbursement is approved or denied.

xi. Where the reimbursement is denied, financial institutions shall provide reasons to the customer for such denial.

xii. Where a customer fails to report an APP fraud incident within seventy-two (72) hours of occurrence, and without reasonable justification, the financial institution may not be obligated to provide reimbursement, except where internal control failures or staff negligence contributed to the fraud. For the purpose of this provision, “reasonable justification” may include, but is not limited to, circumstances beyond the control of the

customer such as illness, force majeure events, time of becoming aware of the fraud, security constraints, or demonstrable unavailability of reporting channels.

xiii. Failure to initiate or conclude the investigation within the stipulated timelines without reasonable justification may constitute a breach of consumer protection obligations and attract appropriate regulatory sanctions.

8.0. REIMBURSEMENT

Banks and OFIs shall implement a fair, timely, and transparent reimbursement process for victims of APP fraud, subject to the following principles:

i. Customers who are victims of APP fraud shall be eligible for reimbursement, subject to the investigation outcomes.

ii. Reimbursement, where applicable, shall be made within forty-eight (48) hours from the conclusion of a documented APP fraud investigation.

iii. Where an APP fraud incident involves more than one financial institution, the originating financial institution shall, commence investigation immediately and notify the other institution(s) involved within 30 minutes of receiving the customer's complaint.

iv. In the course of the investigation and data sharing, all exchange of customer information shall comply with the Nigeria Data Protection Act, 2023.

v. The institutions involved shall conduct a joint investigation to determine the lapses, amount lost or unrecoverable, modalities for joint reimbursement and measures for mitigating future occurrence and losses.

vi. The affected institutions shall make the reimbursement within sixteen (16) working days from the date the incident was first reported.

EXPOSURE DRAFT

vii. Institutions with inadequate fraud detection systems that fail to flag or freeze such proceeds shall be debited for the total exposure amount.

viii. Where the institutions fail to reach a resolution within the period stipulated with respect to Section 7.0 (ix), the complaint shall be escalated to the Consumer Protection and Financial Inclusion Department of the CBN, which shall issue its decision on the complaint to the concerned institutions.

ix. Where neither the sending nor receiving institution is at fault and the customer is eligible for reimbursement, the financial institutions involved shall reimburse the customer (except where Section 8.2 applies), with the cost shared equally between the institutions.

8.1 Eligibility for Reimbursement

A customer shall be considered eligible for reimbursement where:

i. The customer authorised the transaction under false pretence by another party and had no cause to suspect fraud;

ii. The customer reported the APP fraud within seventy-two hours (72) and cooperated with the investigation;

iii. There is no evidence of negligence, collusion, or criminal intent on the part of the customer; and

iv. The financial institution failed to implement appropriate fraud detection, warning, or verification protocols, that could have prevented the transaction.

8.2 Exclusions from Reimbursement

Financial institutions shall not be obligated to reimburse in cases where:

i. The customer acted fraudulently or with negligence;

ii. The customer failed to or delayed reporting the fraud beyond seventy-two (72) hours of occurrence except for reasons highlighted in Section 7.0 (xii); and

EXPOSURE DRAFT

iii. The transaction occurred prior to the effective date of this Guidelines, unless voluntarily applied retroactively.

9.0. REMEDIAL ACTIONS

Financial institutions shall take remedial actions on individuals and accounts used to facilitate APP fraud in line with measures prescribed in extant CBN regulations.

10.0. CONSUMER EDUCATION AND AWARENESS

i. Financial institutions shall ensure that customers are aware of available fraud reporting channels and shall provide clear, accessible, and continuous education on APP fraud risks and reporting procedures.

ii. Financial institution shall carry out quarterly APP fraud awareness campaigns across multiple media and languages.

11.0. DISPUTE RESOLUTION AT THE CENTRAL BANK OF NIGERIA

Where a customer is dissatisfied with the outcome of the resolution, such a customer may escalate the matter to the Director, Consumer Protection and Financial Inclusion Department, CBN and such dispute shall be resolved in line with the extant Consumer Protection Regulations.

12.0. RENDITION OF RETURNS

i. Financial institutions shall submit on a quarterly basis in the prescribed format**:**

a. Return on APP fraud incidents, trends, and remedial actions to the relevant supervisory department in the Bank.
b. Evidence of financial literacy outreach programmes, including the number of consumers reached and the languages used to the Director, Consumer Protection and Financial Inclusion Department.

ii. Financial institutions shall maintain detailed records of APP fraud incidents and make them available to the CBN upon request.

EXPOSURE DRAFT

13.0. SANCTIONS

i. Failure of a financial institution to comply with any of the requirements under this Guidelines constitutes a regulatory breach and shall attract a penalty as may be prescribed by the CBN.

ii. Rendition of false, misleading and/or incomplete information to the CBN shall attract appropriate sanctions including monetary penalties and administrative sanctions on the individual and the bank.

FINANCIAL POLICY & REGULATION DEPARTMENT
NOVEMBER 2025

EXPOSURE DRAFT